ROB BONTA
Attorney General of California
MARK R. BECKINGTON
Supervising Deputy Attorney General
ROBERT L. MEYERHOFF
Deputy Attorney General
State Bar No. 298196
300 South Spring Street, Suite 1702
Los Angeles, CA 90013-1230
Telephone: (213) 269-6177
Fax: (916) 731-2144
E-mail: Robert.Meyerhoff@doj.ca.gov
Attorneys for Rob Bonta in his Official Capacity as Attorney of the State of California

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETCHOICE, Plaintiff, **v.** **ROB BONTA, ATTORNEY GENERAL OF THE STATE OF CALIFORNIA, in his official capacity,** Defendant.	Case No: 5:25-cv-03178-BFL **DECLARATION OF SERGE EGELMAN, PH.D. IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION** Date: June 26, 2025 Time: 9:00am Courtroom: 1, 5th Floor Judge: Hon. Beth Labson Freeman Trial Date: n/a Action Filed: April 9, 2025

I, Serge Egelman, Ph.D., declare and state as follows:

1. I submit this declaration in support of Defendant's Opposition to Plaintiff's Motion for a Second Preliminary Injunction.

2. I have been retained by the Office of the Attorney General of the California Department of Justice to provide expert opinions on the existing efforts by online marketplaces to track sales and on the ways in which online marketplaces are already incentivized to collect sales information.

3. This declaration is based on my own personal knowledge and experience, and if I am called to testify as a witness, I could and would testify competently to the truth of the matters discussed in this declaration.

BACKGROUND & QUALIFICATIONS

4. I am the Research Director of the Usable Security & Privacy Group at the International Computer Science Institute (ICSI), which is a non-profit research institute affiliated with the University of California, Berkeley. I also hold a position as a research scientist within the Electrical Engineering and Computer Sciences (EECS) Department at the University of California, Berkeley. I received my Ph.D. from Carnegie Mellon University's School of Computer Science. My research has been cited over 14,000 times, and my h-index—the most common metric for scientific impact[1]—is over 50.[2]

5. I have been performing research into online privacy for over twenty years. My research focuses on the interplay of online privacy, computer security, and human factors. In short, I study: consumer privacy and security decision making; consumer privacy preferences; privacy and security expectations; and how those expectations comport with reality (e.g., by performing technical analyses of online services and other software to examine privacy and security practices). This research involves both technical knowledge to build tools for use in measurement studies (e.g., observational studies of how user data is collected and shared in practice), as well as a deep understanding of how to apply social science methodologies (e.g.,

[1] J.E. Hirsch. "An Index to Quantify an Individual's Scientific Research Output," *Proc. Natl. Acad. Sci.* U.S.A. 102 (46) 16569-16572, https://doi.org/10.1073/pnas.0507655102 (2005).

[2] https://scholar.google.com/citations?user=WN9t4n0AAAAJ&hl=en

human subjects research, surveys, interviews, randomized controlled trials, etc.). I have served as an invited expert for several web standards efforts that pertained to privacy and security, and have received over a dozen awards from the research community (including: privacy research awards from two European data protection authorities, AEPD in Spain and CNIL in France; the USENIX Security Symposium Distinguished Paper Award, from one of the top academic computer security conferences; the Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies; and seven paper awards from the ACM Special Interest Group on Computer-Human Interaction [SIGCHI], the top human-computer interaction conference). I have also been repeatedly invited to speak at the FTC's annual "PrivacyCon" event based on my laboratory's research.

6. Over the past decade, my laboratory has been studying the mobile app ecosystem, which has included building tools to detect when personal information is accessed by mobile apps and the third parties with whom they share it. We have used these tools in peer-reviewed published research studies about consumer privacy, including examining mobile apps' compliance with various privacy regulations and platform policies.

7. One research study performed by my laboratory demonstrated that a majority of child-directed Android apps appeared to be violating COPPA,[3] which led to major policy shifts by both Google and Apple, makers of the two leading mobile platforms. I have since been invited to give keynotes at several international conferences on child development and technology as an expert on online privacy as it pertains to children. I have also testified before the U.S. Senate on how COPPA can be improved to match the realities of modern technology, and have been asked to provide feedback on draft legislation from members of both houses of Congress.

8. My *curriculum vitae*, which sets forth my experience and credentials more fully, is attached as Exhibit A.

9. I have testified as an expert in the following cases:

[3] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale.* Proceedings on Privacy Enhancing Technologies (PoPETS), 2018(3):63–83.

- *Garner v. Amazon.com, Inc.*, Case No. 2:21-cv-00750 (W.D. Wash.)
- *Lopez et al. v. Apple, Inc.*, Case No. 4:19-cv-04577-JSW (N.D. Cal.)
- *Martinez et al. v. D2C, LLC d/b/a UNIVISION NOW*, Case No. 1:23-cv-21394-RNS (S.D. Fla.).
- *Bloom v. Zuffa LLC*, Case No. 2:22-cv-00412-RFB-BNW (D. Nev.)
- *Clark, et. al. v. Yodlee, Inc.*, Case No: 3:20-cv-05991-SK (N.D. Cal.).
- *Czarnionka v. The Epoch Times Association, Inc.*, Case No. 1:22-cv-6348 (S.D.N.Y.)
- *Frasco v. Flo Health, et al.*, Case No. 3:21-cv-00757 (N.D. Cal.).
- *Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, Case No. 20-cv-03842-JST (N.D. Cal. 2021)
- *District of Columbia v. Town Sports International*, *LLC*, Case No. 2020 CA 003691 B (D.C. Sup. Ct. 2020)
- *In re Vizio, Inc., Consumer Privacy Litig*., 238 F. Supp. 3d 1204, (C.D. Cal. 2017)
- *In re Linkedin User Privacy Litigation*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013)
- *In re Netflix Privacy Litigation*, Case No.: 5:11-CV-00379 EJD (N.D. Cal. 2012)

10. I am being compensated in the above-entitled case at an hourly rate of $400/hour for preparing this declaration. My compensation is not in any way dependent on the outcome of this or any related proceeding.

11. The opinions in this declaration are my expert opinions, which are based on my education and training, my peer-reviewed published research and the research of others, my knowledge of relevant technologies (including my reading of the public technical documents offered by NetChoice's members about their capabilities), as well as my reading of the legislation.

12. I have reviewed SB 1144 and in my expert opinion it does not create unduly onerous compliance requirements for NetChoice's members; in most cases, NetChoice's members already collect the data necessary for compliance.

EXISTING EFFORTS BY ONLINE MARKETPLACES TO TRACK SALES

13. From my understanding of the law, online marketplaces would be required to track listings and then collect and verify information from high-volume sellers, amongst other requirements. Online marketplaces, including those run by NetChoice's members, already have mechanisms in place to collect and verify this information, and thus compliance would not be unduly burdensome.

14. Online marketplaces that process payments have been collecting this information for many years. For example, eBay, a NetChoice member, requires sellers to provide tax information so that eBay can perform withholding on their behalf.[4] Amazon, another NetChoice member, similarly performs tax withholding on the seller's behalf, and therefore already collects sellers' identification information, tax information, and bank account information.[5]

15. While other online marketplaces that do not process payments do not—to my knowledge—collect sellers' taxpayer information and banking information, they nonetheless collect sellers' identities and verify their email addresses. Thus, using these online marketplaces' existing mechanisms for monitoring listings and identifying sellers could be easily modified to meet the law's new compliance requirements.

16. As an example, consider Facebook Marketplace, a service of NetChoice member Meta, which is used as an example in NetChoice's Motion for Preliminary Injunction.[6] Facebook Marketplace allows sellers to list items and facilitates communication with potential buyers, but sales are ultimately completed off of the platform (e.g., meeting a buyer in person and then paying via cash). While NetChoice contends that "they have no realistic way to track which items end up being sold (much less where they are sold, to whom, or for how much)," this is contradicted by Facebook Marketplace's user interface: when a sale is completed, the seller is encouraged to mark the item as sold in order to remove the listing (Figure 1). Upon doing this, Facebook Marketplace asks the seller a series of follow-up questions, including the identity of the buyer and the final sales price (Figure 2).

[4] https://www.ebay.com/sellercenter/resources/tax-information
[5] https://www.amazon.com/gp/help/customer/display.html?nodeId=202211260
[6] Plaintiff NetChoice's Notice of Motion and Motion for Preliminary Injunction at 8.

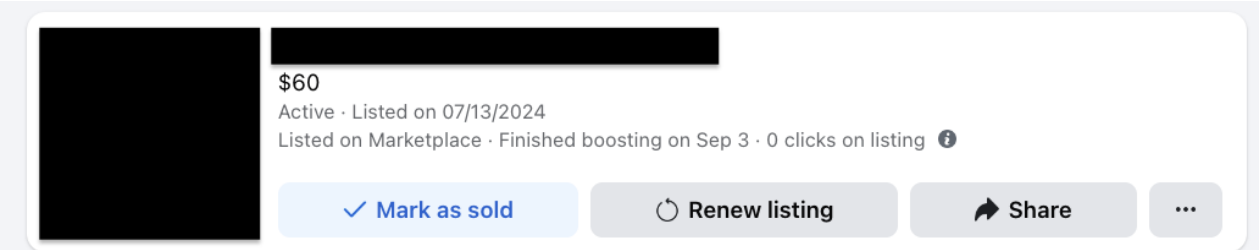

Figure 2: Screenshot from Facebook Marketplace, in which sellers are encouraged to mark items as sold in order to remove the listings.

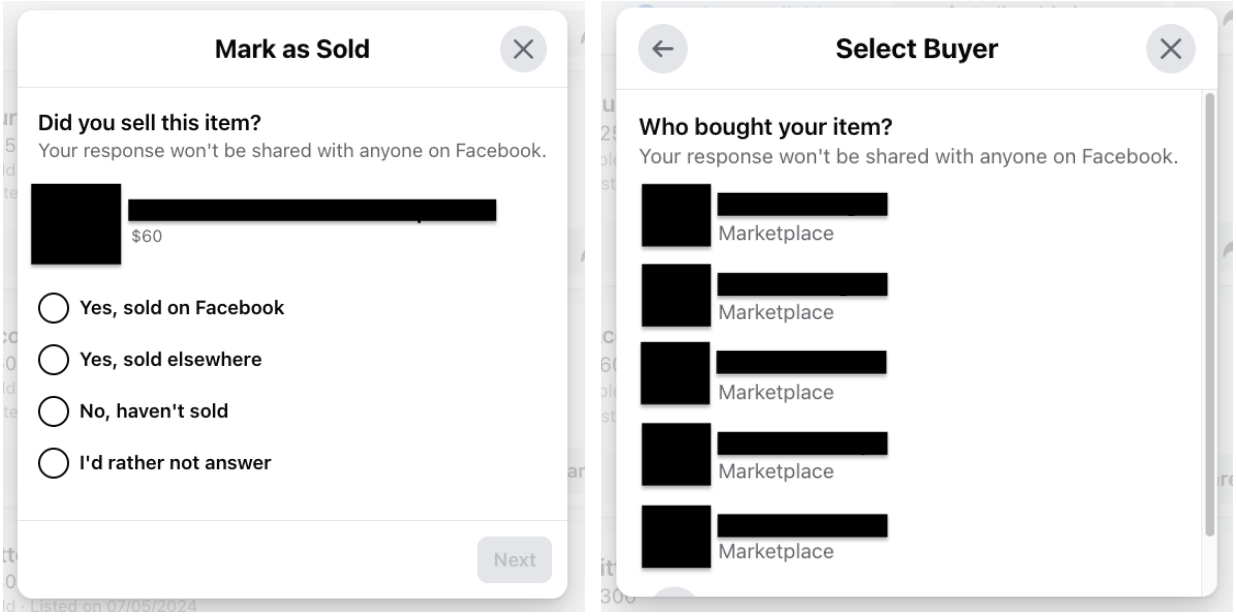

Figure 1: Upon marking a listing as "sold," the seller is asked additional questions about the transaction (left), which includes identifying the Facebook profile of the buyer (right).

17. Because Meta requires all buyers and sellers of Facebook Marketplace to be registered Facebook users (i.e., buyers must have Facebook profiles in order to message sellers), any transaction that was facilitated using Facebook Marketplace will involve a readily identifiable seller. For example, when Meta asks the seller to identify the ultimate buyer, they are able to offer a list of Facebook profiles from which to choose because Meta keeps records of precisely which Facebook users viewed the listing and messaged the seller.

18. If the Facebook Marketplace listing does lead to a sale, the buyer would have had to have had a Facebook profile in order to contact the seller, and thus Meta readily has access to information about both the buyer's and seller's identities, as well as details about the listing (e.g., price).[7] Moreover, the existing mechanisms used to support this functionality could be easily augmented to solicit additional transaction information from high-volume sellers.

19. Thus, it is demonstrably false to state that Meta could not "realistically" collect this information when this is precisely the type of information that Meta *already* collects.

20. While I use Meta as an example here, based on my examination of the websites of Nextdoor and OfferUp (as of May 8, 2025), two other NetChoice members that NetChoice offers as examples of online marketplaces that would allegedly be unduly burdened by the law's record-keeping requirements, this same logic also applies to them.[8] From my examinations of their websites, it is my understanding that both platforms require both buyers and sellers to register accounts with the marketplaces,[9] and that email addresses are verified as part of this registration process. Thus, for any sale that is facilitated on these platforms, the online marketplace would have access to verified contact information for both the seller and any potential buyers.

21. Moreover, after a completed sale, since the seller will need to interact with the online marketplace to mark the item as sold in order to remove the listing, this presents an ideal opportunity for the marketplace to ask the seller questions about the sale (as Meta already does).

ONLINE MARKETPLACES ARE ALREADY INCENTIVIZED TO COLLECT THE REQUIRED INFORMATION

22. In addition to already collecting identifiable information about their users (e.g., as part of account registration, tax withholding, etc.), online marketplaces already collect and retain transaction data because they are incentivized to do so.

[7] As an aside, from having personally used Facebook Marketplace, I can state that listing data is very clearly retained for *years* by Meta.

[8] Plaintiff NetChoice's Notice of Motion and Motion for Preliminary Injunction at 8.

[9] On Nextdoor, a valid user account is required to view listings, whereas on OfferUp, similar to Facebook Marketplace, a valid user account is required to contact the seller (a necessary step when making a purchase).

23. Specifically, online marketplaces regularly collect detailed transaction data to both support desirable features for their users and to analyze, improve, and better monetize their products. For example, all of the online marketplaces that Plaintiffs name in their Motion for Preliminary Injunction all retain listings for months, if not years.[10] For example, my Craigslist account shows listings going back more than three years (i.e., details about the item, asking price, when it was listed/removed, etc.); Facebook Marketplace,[11] Nextdoor,[12] and OfferUp[13] all retain detailed transaction data. All of these online marketplaces retain detailed transaction data because they recognize that being able to search and examine prior transactions is a feature that is desired by their users.

24. Moreover, beyond providing user functionality, online marketplaces are incentivized to collect transaction data because they can glean it for insights about their platforms that can later be monetized. For example, many of these marketplaces are monetized by paid premium features, such as sellers paying to have their listings prioritized in search results.[14] To sell consumers (i.e., sellers) on these paid premium features, online platforms market them as increasing sales by some quantifiable measure. For example:

- Facebook Marketplace: "Sellers who boost get 2.5x more listing views on average than those who don't."[15]
- OfferUp: "Promoted items are twice as likely to sell because they get more exposure at the top of the feed. More exposure helps attract more potential buyers."[16]

25. While not every online marketplace offers these types of paid premium features, all of them are incentivized to collect and retain transaction data for their own analytics purposes.

---

[10] Plaintiff NetChoice's Notice of Motion and Motion for Preliminary Injunction at 8.

[11] As noted earlier, my personal Facebook Marketplace account shows completed listings going back more than a year.

[12] Nextdoor's documentation indicates that it also retains listing information after transactions are completed: https://help.nextdoor.com/s/article/How-to-manage-your-listings-in-For-Sale-and-Free?language=en_US

[13] OfferUp's documentation indicates that it also retains listing information after transactions are completed: https://help.business.offerup.com/hc/en-us/articles/30034350492820-Manage-listings-with-OfferUp-Business-Portal

[14] https://www.facebook.com/business/help/304288543633513?id=150605362430228

[15] https://www.facebook.com/marketplace/learn-more/selling/boosted-listings/

[16] https://help.offerup.com/hc/en-us/articles/360052029431-About-Promote-Plus

This type of data is routinely collected by online services, where it is then used for analysis, and the insights drawn from it are used to guide everything from product design to pricing strategy.

OPINIONS

26. In conclusion, it is my opinion that the compliance burdens that AB 1144 imposes on online marketplaces are not unduly burdensome: many of the records that online marketplaces would be required to collect are already being collected, the mechanisms by which to collect them already exist, and in many cases companies are already incentivized to collect this type of data.

I declare under penalty of perjury that the foregoing is true and correct. Executed on this 15th day of May, 2025 in Berkeley, California.

Serge Egelman, Ph.D.

EXHIBIT A

SergeEgelman

contact
2150 Shattuck Avenue
Suite 250
Berkeley, CA 94704
USA

egelman@cs.berkeley.edu

education

2009	**PhD** in Computation, Organizations, and Society School of Computer Science	Carnegie Mellon University
2004	**BS** in Computer Engineering School of Engineering and Applied Science	University of Virginia

experience

	AppCensus, Inc.	San Francisco, CA
2022–Now	Chief Scientist / Co-Founder	
2019–2022	CTO / Co-Founder	
	International Computer Science Institute	Berkeley, California
2016–Now	Research Director, Usable Security & Privacy Group	
2013–2016	Senior Researcher, Networking and Security Group	
	University of California, Berkeley	Berkeley, California
2011–Now	Research Scientist, Electrical Engineering and Computer Sciences	
	National Institute of Standards and Technology	Gaithersburg, Maryland
2010–2011	Research Scientist, Visualization and Usability Group	
	Brown University	Providence, Rhode Island
2009-2010	Postdoctoral Researcher, Computer Science Department	
	Microsoft Research	Redmond, Washington
2008	Research Intern, Security and Privacy Group	
2008	Research Intern, VIBE Group	
	PARC	Palo Alto, California
2006	Research Intern, Computer Science Laboratory	

publications*

refereed journal publications

The Effect of Platform Policies on App Privacy Compliance: A Study of Child-Directed Apps
Alomar, N., Reardon, J., Girish, A., Vallina-Rodriguez, N., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *2025.2 (2025).*

"Protect Me Tomorrow": Commitment Nudges to Remedy Compromised Passwords
Peer, E., Frik, A., Gilsenan, C., and Egelman, S. ACM Trans. Comput.-Hum. Interact. *(Aug. 2024). Association for Computing Machinery.*

*Over 13,000 citations and h-index=53: https://scholar.google.com/citations?hl=en&user=WN9t4n0AAAAJ

The Medium is the Message:
How Secure Messaging Apps Leak Sensitive Data to Push Notification Services
Samarin, N., Sanchez, A., Chung, T., Juleemun, A. D. B., Gilsenan, C., Merrill, N., Reardon, J., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *2024.4 (2024) pp. 967–982.*

A Model of Contextual Factors Affecting Older Adults'
Information-Sharing Decisions in the U.S.
Frik, A., Bernd, J., and Egelman, S. ACM Transactions on Computer-Human Interaction *30.1 (Apr. 2023). Association for Computing Machinery.*

Lessons in VCR Repair:
Compliance of Android App Developers with the California Consumer Privacy Act (CCPA)
Samarin, N., Kothari, S., Siyed, Z., Bjorkman, O., Yuan, R., Wijesekera, P., Alomar, N., Fischer, J., Hoofnagle, C., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *3 (2023).*

Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps
Alomar, N., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *4 (2022) pp. 250–273.*

Data Collection Practices of Mobile Applications Played by Preschool-Aged Children
Zhao, F., Egelman, S., Weeks, H. M., Kaciroti, N., Miller, A. L., and Radesky, J. S. JAMA Pediatrics *174.12 (Dec. 2020).*

Nudge Me Right: Personalizing Online Security Nudges to People's Decision-Making Styles
Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., and Frik, A. Computers in Human Behavior *109 (Aug. 2020).*

Disaster Privacy/Privacy Disaster
Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., and Egelman, S. Journal of the Association for Information Science and Technology *(Mar. 2020).*

Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps
Bamberger, K. A., Egelman, S., Han, C., Elazari, A., and Reyes, I. Berkeley Technology Law Journal *35 (2020).*

The Price is (Not) Right: Comparing Privacy in Free and Paid Apps
Han, C., Reyes, I., Feal, Á., Reardon, J., Wijesekera, P., Vallina-Rodriguez, N., Elazari, A., Bamberger, K. A., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *3 (2020).*

Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants
Tabassum, M., Kosiński, T., Frik, A., Malkin, N., Wijesekera, P., Egelman, S., and Lipford, H. R. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technoligies (IMWUT) *3.4 (Dec. 2019). Association for Computing Machinery.*

Privacy Attitudes of Smart Speaker Users
Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Wagner, D., and Egelman, S. Proceedings on Privacy Enhancing Technologies *2019.4 (2019).*

"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale
Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., and Egelman, S. Proceedings on Privacy Enhancing Technologies *2018.3 (2018) pp. 63–83.* **Caspar Bowden PET Award**

A Usability Evaluation of Tor Launcher
Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., and Wagner, D. Proceedings on Privacy Enhancing Technologies *2017.3 (2017) pp. 87–106.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. Information Systems Research *22.2 (2011) pp. 254–268.* **AIS Best Publication of 2011 Award / INFORMS Best Published Paper Award (2012)**

P3P Deployment on Websites
Cranor, L. F., Egelman, S., Sheng, S., McDonald, A. M., and Chowdhury, A. Electronic Commerce Research and Applications *7.3 (2008) pp. 274–293.*

The Real ID Act: Fixing Identity Documents with Duct Tape
Egelman, S., and Cranor, L. F. I/S: A Journal of Law and Policy for the Information Society *2.1 (2006) pp. 149–183.*

refereed conference publications

Security and Privacy Failures in Popular 2FA Apps
Gilsenan, C., Shakir, F., Alomar, N., and Egelman, S. Proceedings of the 32nd USENIX Security Symposium *(USENIX Security '23), 2023.*

In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes
Girish, A., Hu, T., Prakash, V., Dubois, D. J., Matic, S., Huang, D. Y., Egelman, S., Reardon, J., Tapiador, J., Choffnes, D., and Vallina-Rodriguez, N. Proceedings of the 2023 ACM on Internet Measurement Conference *(IMC '23), 2023, New York, NY, USA.*

Log: It's Big, It's Heavy, It's Filled with Personal Data!
Measuring the Logging of Sensitive Information in the Android Ecosystem
Lyons, A., Gamba, J., Shawaga, A., Reardon, J., Tapiador, J., Egelman, S., and Vallina-Rodriguez, N. Proceedings of the 32nd USENIX Security Symposium *(USENIX Security '23), 2023.*

Can Humans Detect Malicious Always-Listening Assistants?
A Framework for Crowdsourcing Test Drives
Malkin, N., Wagner, D., and Egelman, S. Proceedings of the ACM Conference On Computer-Supported Cooperative Work And Social Computing *(CSCW '22), 2022, New York, NY, USA.*

Runtime Permissions for Privacy in Proactive Intelligent Assistants
Malkin, N., Wagner, D., and Egelman, S. Eighteenth Symposium on Usable Privacy and Security *(SOUPS 2022), 2022.*

"You've Got Your Nice List of Bugs, Now What?" Vulnerability Discovery and Management Processes in the Wild
Alomar, N., Wijesekera, P., Qiu, E., and Egelman, S. Proceedings of the Sixteenth Symposium on Usable Privacy and Security *(SOUPS 2020), 2020.*

Actions Speak Louder than Words: Entity-Sensitive Privacy Policy and Data Flow Analysis with PoliCheck
Andow, B., Mahmud, S. Y., Whitaker, J., Enck, W., Reaves, B., Singh, K., and Egelman, S. 29th USENIX Security Symposium *(USENIX Security '20), 2020, Boston, MA.*

Don't Accept Candies from Strangers: An Analysis of Third-Party Mobile SDKs
Feal, Á., Gamba, J., Tapiador, J., Wijesekera, P., Reardon, J., Egelman, S., and Vallina-Rodriguez, N. International Conference on Computers, Privacy and Data Protection *(CPDP '20), 2020.*

A Qualitative Model of Older Adults' Contextual Decision-Making About Information Sharing
Frik, A., Bernd, J., Alomar, N., and Egelman, S. Workshop on the Economics of Information Security *(WEIS '20), 2020.*

Empirical Measurement of Systemic 2FA Usability
Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., and Egelman, S. Proceedings of the 29th USENIX Security Symposium *(USENIX Security '20), 2020.*

A Promise Is A Promise: The Effect of Commitment Devices on Computer Security Intentions
Frik, A., Malkin, N., Harbach, M., Peer, E., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '19), 2019.*

Privacy and Security Threat Models and Mitigation Strategies of Older Adults
Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F., and Egelman, S. Proceedings of the 15th Symposium on Usable Privacy and Security *(SOUPS '19), 2019, Berkeley, CA, USA.*

Information Design in An Aged Care Context
Nurgalieva, L., Frik, A., Ceschel, F., Egelman, S., and Marchese, M. Proceedings of the 13th International Conference on Pervasive Computing Technologies for Healthcare *(PervasiveHealth '19), 2019, New York, NY, USA.*

50 Ways to Leak Your Data:
An Exploration of Apps' Circumvention of the Android Permissions System
Reardon, J., Feal, A., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S. Proceedings of the 24th USENIX Security Symposium *(USENIX Security '19), 2019, Berkeley, CA, USA.* **USENIX Security Distinguished Paper Award / AEPD Emilio Aced Personal Data Protection Research Award / CNIL-INRIA Privacy Award**

An Experience Sampling Study of User Reactions to Browser Warnings in the Field
Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.*

Contextualizing Privacy Decisions for Better Prediction (and Protection)
Wijesekera, P., Reardon, J., Reyes, I., Tsai, L., Chen, J.-W., Good, N., Wagner, D., Beznosov, K., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.* **SIGCHI Honorable Mention Award**

Let's go in for a closer look: Observing passwords in their natural habitat
Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Forget, A. Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '17), 2017, New York, NY, USA.*

Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences
Tsai, L., Wijesekera, P., Reardon, J., Reyes, I., Egelman, S., Wagner, D., Good, N., and Chen, J.-W. Proceedings of the 13th Symposium on Usable Privacy and Security *(SOUPS '17), 2017.*

The Feasibility of Dynamically Granted Permissions:
Aligning Mobile Privacy with User Preferences
Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., and Beznosov, K. Proceedings of the 2017 IEEE Symposium on Security and Privacy *(Oakland '17), 2017.*

Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes
Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., and Telang, R. Proc. of the 12th Symposium on Usable Privacy and Security *(SOUPS '16), 2016.*

Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS)
Egelman, S., Harbach, M., and Peer, E. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens
Harbach, M., Luca, A. D., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking
Harbach, M., Luca, A. D., Malkin, N., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Teaching Privacy Curriculum
Egelman, S., Bernd, J., Friedland, G., and Garcia, D. Proceedings of the 47th ACM technical symposium on Computer Science Education *(SIGCSE '16), 2016.*

Android Permissions Remystified: A Field Study on Contextual Integrity
Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., and Beznosov, K. 24th USENIX Security Symposium *(USENIX Security 15), 2015, Washington, D.C.*

Is This Thing On? Communicating Privacy on Ubiquitous Sensing Platforms
Egelman, S., Kannavara, R., and Chow, R. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)
Egelman, S., and Peer, E. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.* **SIGCHI Honorable Mention Award**

Fingerprinting Web Users through Font Metrics
Fifield, D., and Egelman, S. Proceedings of the 19th international conference on Financial Cryptography and Data Security *(FC'15), 2015.*

Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights
Portnoff, R., Lee, L., Egelman, S., Mishra, P., Leung, D., and Wagner, D. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors
Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., and Wagner, D. Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '14), 2014, New York, NY, USA.*

The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior
Tan, J., Nguyen, K., Theodorides, M., Negron-Arroyo, H., Thompson, C., Egelman, S., and Wagner, D. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '14), 2014, Toronto, Canada.*

The Importance of Being Earnest [in Security Warnings]
Egelman, S., and Schechter, S. Proceedings of the 17th international conference on Financial Cryptography and Data Security *(FC'13), 2013, Okinawa, Japan.*

My Profile Is My Password, Verify Me! The Privacy/Convenience Tradeoff of Facebook Connect
Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection
Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., and Herley, C. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

When It's Better to Ask Forgiveness than Get Permission: Attribution Mechanisms for Smartphone Resources
Thompson, C., Johnson, M., Egelman, S., Wagner, D., and King, J. Proceedings of the Ninth Symposium on Usable Privacy and Security *(SOUPS '13), 2013, Newcastle, United Kingdom.*

Android permissions: user attention, comprehension, and behavior
Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.* **SOUPS Best Paper Award (2012) / SOUPS Impact Award (2017)**

Facebook and privacy: it's complicated
Johnson, M., Egelman, S., and Bellovin, S. M. Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.*

It's all about the Benjamins: Incentivizing users to ignore security advice
Christin, N., Egelman, S., Vidas, T., and Grossklags, J. Proceedings of the 15th international conference on Financial Cryptography and Data Security *(FC'11), 2011, Gros Islet, St. Lucia.*

Oops, I did it again: mitigating repeated access control errors on facebook
Egelman, S., Oates, A., and Krishnamurthi, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.*

Of passwords and people: measuring the effect of password-composition policies
Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.* **SIGCHI Honorable Mention Award**

Timing is everything?: the effects of timing and placement of online privacy indicators
Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions
Schechter, S., Brush, A. J. B., and Egelman, S. Proceedings of the 2009 IEEE Symposium on Security and Privacy *(Oakland '09), 2009, Los Alamitos, CA, USA.*

It's not what you know, but who you know: a social approach to last-resort authentication
Schechter, S., Egelman, S., and Reeder, R. W. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

Crying wolf: an empirical study of SSL warning effectiveness

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. Proceedings of the 18th USENIX Security Symposium *(SSYM'09), 2009, Montreal, Canada.*

Family accounts: a new paradigm for user accounts within the home environment
Egelman, S., Brush, A. J. B., and Inkpen, K. M. Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work *(CSCW '08), 2008, San Diego, CA, USA.*

You've Been Warned: An empirical study of the effectiveness of browser phishing warnings
Egelman, S., Cranor, L. F., and Hong, J. CHI '08: Proceeding of The 26th SIGCHI Conference on Human Factors in Computing Systems *(CHI '08), 2008, Florence, Italy.* **SIGCHI Honorable Mention Award**

Phinding Phish: Evaluating Anti-Phishing Tools
Zhang, Y., Egelman, S., Cranor, L. F., and Hong, J. Proceedings of the 14th Annual Network & Distributed System Security Symposium *(NDSS '07), 2007, San Diego, CA.*

Power Strips, Prophylactics, and Privacy, Oh My!
Gideon, J., Egelman, S., Cranor, L., and Acquisti, A. Proceedings of the Second Symposium on Usable Privacy and Security *(SOUPS '06), 2006, Pittsburgh, PA.*

An analysis of P3P-enabled web sites among top-20 search results
Egelman, S., Cranor, L. F., and Chowdhury, A. Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet *(ICEC '06), 2006, Fredericton, New Brunswick, Canada.*

refereed workshop publications

Challenges in Inferring Privacy Properties of Smart Devices:
Towards Scalable Multi-Vantage Point Testing Methods
Girish, A., Prakash, V., Egelman, S., Reardon, J., Tapiador, J., Huang, D. Y., Matic, S., and Vallina-Rodriguez, N. Proceedings of the 3rd International CoNEXT Student Workshop *(CoNEXT-SW '22), 2022, Rome, Italy.*

Identifying and Classifying Third-Party Entities in Natural Language Privacy Policies
Hosseini, M. B., Pragyan, K., Reyes, I., and Egelman, S. Proceedings of the Second Workshop on Privacy in Natural Language Processing *(PrivateNLP '20), 2020.*

Do You Get What You Pay For? Comparing The Privacy Behaviors of Free vs. Paid Apps
Han, C., Reyes, I., On, A. E. B., Reardon, J., Feal, A., Bamberger, K. A., Egelman, S., and Vallina-Rodriguez, N. The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Privacy Controls for Always-Listening Devices
Malkin, N., Egelman, S., and Wagner, D. Proceedings of the New Security Paradigms Workshop *(NSPW '19), 2019, San Carlos, Costa Rica.*

On The Ridiculousness of Notice and Conset: Contradictions in App Privacy Policies
Okoyomon, E., Samarin, N., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., Reyes, I., Feal, A., and Egelman, S. The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Better Late(r) than Never: Increasing Cyber-Security Compliance by Reducing Present Bias
Frik, A., Egelman, S., Harbach, M., Malkin, N., and Peer, E. Workshop on the Economics of Information Security *(WEIS '18), 2018.*

"What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the U.S.
Malkin, N., Bernd, J., Johnson, M., and Egelman, S. Proceedings of the European Workshop on Usable Security *(EuroUSEC '18), 2018.*

Personalized Security Messaging: Nudges for Compliance with Browser Warnings
Malkin, N., Mathur, A., Harbach, M., and Egelman, S. Proceedings of the European Workshop on Usable Security *(EuroUSEC '17), 2017.*

"Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations
Reyes, I., Wijesekera, P., Razaghpanah, A., Reardon, J., Vallina-Rodriguez, N., Egelman, S., and Kreibich, C. The Workshop on Technology and Consumer Protection *(ConPro '17), 2017.*

Information Disclosure Concerns in The Age of Wearable Computing

Lee, L. N., Lee, J. H., Egelman, S., and Wagner, D. Proceedings of the NDSS Workshop on Usable Security *(USEC '16), 2016.*

The Myth of the Average User:
Improving Privacy and Security Systems through Individualization
Egelman, S., and Peer, E. Proceedings of the 2015 Workshop on New Security Paradigms *(NSPW '15), 2015, Twente, The Netherlands.*

Teaching Privacy: What Every Student Needs to Know
Friedland, G., Egelman, S., and Garcia, D. Proceedings of the 46th SIGCSE technical symposium on computer science education *(Workshop), 2015.*

U-PriSM 2: The Second Usable Privacy and Security for Mobile Devices Workshop
Chiasson, S., Crawford, H., Egelman, S., and Irani, P. Proc. of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services *(MobileHCI '13), 2013, Munich, Germany.*

Markets for Zero-day Exploits: Ethics and Implications
Egelman, S., Herley, C., and Oorschot, P. C. van Proceedings of the 2013 Workshop on New Security Paradigms Workshop *(NSPW '13), 2013, Banff, Alberta, Canada.*

Choice Architecture and Smartphone Privacy: There's A Price for That
Egelman, S., Felt, A. P., and Wagner, D. The 2012 Workshop on the Economics of Information Security *(WEIS '12), 2012, Berlin, Germany.*

How Good Is Good Enough? The sisyphean struggle for optimal privacy settings
Egelman, S., and Johnson, M. Proceedings of the Reconciling Privacy with Social Media Workshop *(CSCW '12 Workshop), 2012, Seattle, WA.*

It's Not Stealing if You Need It: A Panel on the Ethics of Performing Research Using Public Data of Illicit Origin
Egelman, S., Bonneau, J., Chiasson, S., Dittrich, D., and Schechter, S. Proceedings of the 16th International Conference on Financial Cryptography and Data Security *(FC'12), 2012.*

How to ask for permission
Felt, A. P., Egelman, S., Finifter, M., Akhawe, D., and Wagner, D. Proceedings of the 7th USENIX conference on Hot Topics in Security *(HotSec'12), 2012, Bellevue, WA.*

I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns
Felt, A. P., Egelman, S., and Wagner, D. Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices *(SPSM '12), 2012, Raleigh, North Carolina, USA.*

Toward Privacy Standards Based on Empirical Studies
Egelman, S., and McCallister, E. The Workshop on Web Tracking and User Privacy *(W3C Workshop), 2011, Princeton, NJ.*

Please Continue to Hold: An Empirical Study on User Tolerance of Security Delays
Egelman, S., Molnar, D., Christin, N., Acquisti, A., Herley, C., and Krishnamurthi, S. Workshop on the Economics of Information Security (WEIS '10) *(WEIS '10), 2010, Cambridge, MA.*

Tell Me Lies: A Methodology for Scientifically Rigorous Security User Studies
Egelman, S., Tsai, J., and Cranor, L. F. Proceedings of the Workshop on Studying Online Behavior *(CHI '10 Workshop), 2010, Atlanta, GA.*

This is Your Data on Drugs: Lessons Computer Security Can Learn from the Drug War
Molnar, D., Egelman, S., and Christin, N. Proceedings of the 2010 Workshop on New Security Paradigms *(NSPW '10), 2010, Concord, Massachusetts, USA.*

Security user studies: methodologies and best practices
Egelman, S., King, J., Miller, R. C., Ragouzis, N., and Shehan, E. CHI '07 Extended Abstracts on Human Factors in Computing Systems *(CHI EA '07), 2007, San Jose, CA, USA.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. Proceedings of the 2007 Workshop on the Economics of Information Security *(WEIS '07), 2007, Pittsburgh, PA, USA.*

Studying the Impact of Privacy Information on Online Purchase Decisions
Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. Proceedings of the Workshop on Privacy and HCI: Methodologies for Studying Privacy Issues *(CHI '06 Workshop), 2006, Montreal, Canada.*

book chapters and magazine articles

50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System
Reardon, J., Feal, Á., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S. *;login:* 2019, USENIX Association.

Predicting Privacy and Security Attitudes
Egelman, S., and Peer, E. *Computers and Society*, 2015, ACM.

Crowdsourcing
Egelman, S., Chi, E., and Dow, S. *Ways of Knowing in HCI*, 2013, Springer.

Helping users create better passwords
Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Lopez, J. *;login:* 2012, USENIX Association.

Suing Spammers for Fun and Profit
Egelman, S. *;login:* 2004, USENIX Association.

Installation
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

User Administration
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

awards and recognition

2024 **2024 Norm Hardy Prize for Advances in Usable Security**
"Protect Me Tomorrow": Commitment Nudges to Remedy Compromised Passwords, with A. Frik, C. Gilsenan, and E. Peer.

2022 **CNIL-INRIA Privacy Award**
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

Emilio Aced Personal Data Protection Research Award
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2020 **Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies**
"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale, with I. Reyes, P. Wijesekera, J. Reardon, A. Elazari, A. Razaghpanah, and N. Vallina-Rodriguez.

2019 **USENIX Security Symposium Distinguished Paper Award**
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2018 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Contextualizing Privacy Decisions for Better Prediction (and Protection), with P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, and K. Beznosov.

2017 **Symposium on Usable Privacy and Security (SOUPS) Impact Award**
Android Permissions: User Attention, Comprehension, and Behavior, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

Elected ACM Senior Member Association for Computing Machinery (ACM)

2016 **Symposium on Usable Privacy and Security (SOUPS) Distinguished Poster Award**
Risk Compensation in Home-User Computer Security Behavior: A Mixed-Methods Exploratory Study, with S. Pearman, A. Kumar, N. Munson, C. Sharma, L. Slyper, L. Bauer, and N. Christin.

SIGCHI Honorable Mention Award (Best Paper Nominee)
Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS), with M. Harbach and E. Peer.

SIGCHI Honorable Mention Award (Best Paper Nominee)
The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens, with M. Harbach and A. De Luca.

SIGCHI Honorable Mention Award (Best Paper Nominee)
Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking, with M. Harbach, A. De Luca, and N. Malkin.

2015 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Scaling the Security Wall: Developing a Security Behavior Intentions Scale, with E. Peer.

2012 **AIS Best Publication of 2011**
The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, with J. Tsai, L. Cranor, and A. Acquisti.

ISR Best Published Paper
The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, with J. Tsai, L. Cranor, and A. Acquisti.

SOUPS Best Paper Award
Android Permissions: User Attention, Comprehension, and Behavior, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

2011 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Of Passwords and People: Measuring the Effect of Password-Composition Policies, with S. Komanduri, R. Shay, P. G. Kelley, M. Mazurek, L. Bauer, N. Christin, and L. F. Cranor.

2008 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings, with L. Cranor and J. Hong.

2006 **Tor Graphical User Interface Design Competition**
Phase 1 Overall Winner, with L. Cranor, J. Hong, P. Kumaraguru, C. Kuo, S. Romanosky, J. Tsai, and K. Vaniea.

Publisher's Clearing House Finalist
I *may* already be a winner.

expert testimony and reports

2024 Expert witness for the plaintiffs in *Garner v. Amazon.com, Inc., No. 2:21-cv-00750 (W.D. Wash.)*. I provided a report and testimony explaining how in-home "virtual personal assistants" work, as well as explaining the associated privacy concerns based on the relevant research literature. Also offered opinions on proper survey methods and HCI research in the context of an expert rebuttal report.

2024 Expert witness for the plaintiffs in *Lopez et al. v. Apple, Inc., No. 4:19-cv-04577-JSW (N.D. Cal.)*. I provided a report explaining how in-home "virtual personal assistants" work, as well as explaining the associated privacy concerns based on the relevant research literature.

2024 Expert witness for the plaintiffs in *Martinez et al. v. D2C, LLC d/b/a UNIVISION NOW, No. 1:23-cv-21394-RNS (S.D. Fla.)*. I provided a report and testimony explaining how the Meta Pixel functions and how it was used to transmit consumers' personally-identifiable information in violation of the Video Privacy Protection Act (VPPA).

2024	Expert witness for the plaintiffs in *Bloom v. Zuffa LLC, No. 2:22-cv-00412-RFB-BNW (D. Nev.)*. I provided a report and testimony explaining how the Meta Pixel functions and how it was used to transmit consumers' personally-identifiable information in violation of the Video Privacy Protection Act (VPPA).
2024	Expert witness for the plaintiffs in *Clark, et. al. v. Yodlee, Inc., No: 3:20-cv-05991-SK (N.D. Cal.)*. I provided a report and testimony explaining basic data protection concepts and consumer privacy expectations.
2024	Independent expert witness appointed by the court in *Czarnionka v. The Epoch Times Association, Inc., No. 1:22-cv-6348 (S.D.N.Y.)*. I was asked to perform a technical analysis to confirm that the terms of the injunctive relief were being followed.
2023-2024	Expert witness for the plaintiffs in *Frasco v. Flo Health, et al., No. 3:21-cv-00757 (N.D. Cal.)*. I provided an expert report and testimony based on my forensic analysis of a mobile app's data collection behaviors (i.e., privacy analysis). I was deposed and also provided rebuttal reports of opposing experts.
2023-2024	Expert witness for the California Department of Justice in *NetChoice, LLC v. Bonta, No. 5:22-cv-08861*. I provided a declaration opposing the motion to dismiss.
2022	Expert witness for the plaintiffs in *Hart, et al. v. TWC Product and Technology LLC, No. 4:20-cv-3842-JST*. I provided a rebuttal report and testimony about mobile app data collection behaviors.
2022	Expert witness for the District of Columbia Office of the Attorney General in *District of Columbia v. Town Sports International LLC*. I provided a rebuttal report and testimony on proper surveying methodology.
2021	Expert witness testifying before the U.S. Senate (Committee on Commerce, Science, and Transportation), hearing on "Protecting Kids Online: Internet Privacy and Manipulative Marketing." Testimony available at: https://www.commerce.senate.gov/2021/5/protecting-kids-online-internet-privacy-and-manipulative-marketing
2017-2019	Expert witness for the plaintiffs in *Vizio, Inc., Consumer Privacy Litigation, No. 8:16-ml-02693-JLS-KES*, assisting with discovery strategy and providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.
2016	Expert witness for the FTC in *FTC v. Amazon.com, Inc., No. C14-1028-JCC*, providing testimony on human-computer interaction (HCI) evaluation methods and critiquing opposing expert's report.
2014-2015	Expert witness for the plaintiffs in *Doe vs. Twitter, Inc., No. CGC-10-503630*, providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.
2014	Expert witness for the plaintiffs in *Levy v. Universal Parking of Florida, LLC No. 13-cv-22122 (S.D. Fla.)*, providing written testimony on basic human-computer interaction concepts as they relate to smartphone usage.
2013	Expert witness for the plaintiffs in *LinkedIn User Privacy Litigation, No. 12-cv-03088-EJD (N.D. Cal.)*, providing explanations of information security concepts and providing original research on users' privacy expectations in order to demonstrate and quantify damages.
2012	Expert witness for the plaintiffs in *Netflix Privacy Litigation, No. 5:11-cv-00379-EJD (N.D. Cal.)*, providing explanations of relevant privacy research and the economics of information privacy in order to quantify damages.

grants awarded

2023–2026	**NSA: Improving Security and Safety of Neural Networks through Robust Training, Noise Augmentation, and Safety Metrics (H98230-23-C-0275)** Co-PI (PI: Michael Mahoney, International Computer Science Institute)	$750,000
2023–2026	**NSF: Measuring, Validating and Improving upon App-Based Privacy Nutrition Labels (CNS-2247951/2247952/2247953)** Principal Investigator (Collaborative with Adam Aviv, George Washington University; Chris Kanich, University of Illinois at Chicago)	$600,000
2022–2025	**NSF: Developer Implementation of Privacy in Software Systems (CCF-2217771/2217772)** Principal Investigator (Collaborative with Primal Wijesekera, International Computer Science Institute; Jon Atwell and Julian Nyarko, Stanford University)	$750,000
2022–2026	**KACST-UCB Center of Excellence for Secure Computing** Senior Personnel (PI: David Wagner, University of California, Berkeley)	$6,460,000
2021–2022	**CITRIS: Auditing the Compliance of California Consumer Privacy Regulations at Scale** Principal Investigator (Collaborative with Zubair Shafiq, University of California, Davis)	$60,000
2019	**Google: ASPIRE: SDK Traffic Identification at Scale** Principal Investigator	$75,000
2018-2022	**NSF: Mobile Dynamic Privacy and Security Analysis at Scale (CNS-1817248)** Principal Investigator	$668,475
2018-2022	**NSF: Contextual Integrity: From Theory to Practice (CNS-1801501/1801307/1801316)** Principal Investigator (Collaborative with Helen Nissenbaum, Cornell University; and Norman Sadeh, Carnegie Mellon University)	$1,199,462
2018-2022	**NSF: Increasing Users' Cyber-Security Compliance by Reducing Present Bias (CNS-1817249)** Principal Investigator	$558,018
2018-2023	**NSA: The Science of Privacy: Implications for Data Usage (H98230-18-D-0006)** Principal Investigator (Co-PI: Michael Tschantz, International Computer Science Institute)	$3,236,424
2018-2019	**DHS: Scaling Contextual Privacy to MDM Environments (FA8750-18-2-0096)** Principal Investigator	$480,000
2018-2019	**Rose Foundation: AppCensus: Mobile App Privacy Analysis at Scale** Principal Investigator (Co-PI: Irwin Reyes, International Computer Science Institute)	$40,000
2018	**Cisco: Access Controls for an IoT World** Principal Investigator	$99,304
2018	**CLTC: Privacy Analysis at Scale** Principal Investigator	$50,000
2018	**CLTC: Secure Internet of Things for Senior Users** Co-PI (PI: Alisa Frik, International Computer Science Institute)	$60,590
2017	**Mozilla: Towards Usable IoT Access Controls in the Home** Principal Investigator	$46,000
2017	**Data Transparency Lab (DTL) / AT&T: Transparency via Automated Dynamic Analysis at Scale** Principal Investigator	$55,865

2017	**CLTC: Secure & Usable Backup Authentication** Co-PI (PI: David Wagner, University of California, Berkeley)	$48,400
2016 - 2017	**NSF: Teaching Security in CSP (CNS-1636590)** Co-PI (PI: Julia Bernd, ICSI)	$200,000
2016 - 2017	**DHS: A Platform for Contextual Mobile Privacy (FA8750-16-C-0140)** Principal Investigator	$664,378
2016 - 2018	**CLTC: The Security Behavior Observatory** Principal Investigator	$195,962
2016	**CLTC: Using Individual Differences to Tailor Security Mitigations** Principal Investigator	$100,000
2015 - 2018	**NSF/BSF: Using Individual Differences to Personalize Security Mitigations (CNS-1528070/BSF-2014626)** Principal Investigator (Collaborative with Eyal Peer, Bar-Ilan University)	$724,732
2015 - 2019	**NSF: Security and Privacy for Wearable and Continuous Sensing Platforms (CNS-1514211/1514457/1513584)** Principal Investigator (Collaborative with David Wagner, University of California, Berkeley; and Franziska Roesner, University of Washington)	$1,200,000
2014 - 2016	**NSF: Teachers' Resources for Online Privacy Education (DGE-1419319)** Co-PI (PI: Gerald Friedland, ICSI)	$300,000
2014 - 2017	**NSA: User Security Behavior** Subcontract (PIs: Lorrie Cranor, Rahul Telang, Alessandro Acquisti, and Nicholas Christin; Carnegie Mellon University)	$200,000
2014	**Google: Improving Security Warnings by Examining User Intent** Principal Investigator	$71,500
2013 - 2015	**NSF: Designing Individualized Privacy and Security Systems (CNS-1343433/1343451)** Principal Investigator (Collaborative with Eyal Peer, Carnegie Mellon University)	$132,620
2013 - 2016	**NSF: A Choice Architecture for Mobile Privacy and Security (CNS-1318680)** Co-PI (PI: David Wagner, University of California, Berkeley)	$500,000
2010	**Google: Designing Usable Certificate Dialogs in Chrome** Principal Investigator	$60,000

patents awarded

2024	Method and Apparatus for Dynamic Outbound Firewalling via Domain Name System (DNS) (US Patent 12,160,407)
2023	Automatic Identification of Applications that Circumvent Permissions and/or Obfuscate Data Flows (US Patent 11,689,551)

professional activities

program committees

2025	USENIX Security Symposium; Workshop on Economics and Information Security (WEIS)
2024	IEEE Security & Privacy; Workshop on Economics and Information Security (WEIS); Contextual Integrity (CI) Symposium
2023	Privacy Enhancing Technologies Symposium (PETS); IEEE Security & Privacy; Workshop on Economics and Information Security (WEIS)
2022	Contextual Integrity (CI) Symposium

2021	Workshop on Economics and Information Security (WEIS)
2020	ACM CCS; Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS); USENIX Security
2019	Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS)
2018	ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS); IEEE Security & Privacy ("Oakland")
2017	ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Privacy Enhancing Technologies Symposium (PETS); New Security Paradigms Workshop (NSPW), **Co-Chair**; Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS)
2016	Workshop on the Economics of Information Security (WEIS), **Chair**; New Security Paradigms Workshop (NSPW), **Co-Chair**; ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Symposium on Usable Privacy and Security (SOUPS); ACM WWW; Financial Cryptography and Data Security; Privacy Enhancing Technologies Symposium (PETS)
2015	Symposium on Usable Privacy and Security (SOUPS); USENIX Security; ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on the Economics of Information Security (WEIS); ACM WWW; Financial Cryptography and Data Security
2014	ACM SIGCHI (Human Factors in Computing Systems); Financial Cryptography and Data Security; ACM WWW; Privacy Enhancing Technologies Symposium (PETS)
2013	ACM SIGCHI (Human Factors in Computing Systems); Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Anti-Phishing Working Group eCrime Researchers Summit
2012	Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW)
2011	Symposium On Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Computers, Freedom, and Privacy (CFP) Conference (poster session co-chair); Software and Usable Security Aligned for Good Engineering (SAUSAGE) Workshop, **Co-Chair**
2010	Symposium On Usable Privacy and Security (SOUPS)
2008	Conference on Information and Knowledge Management (CIKM)
2007	ACM SIGCHI Workshop - Security User Studies: Methodologies and Best Practices; Anti-Phishing Working Group eCrime Researchers Summit (poster session co-chair)
2006	Computers, Freedom, and Privacy (CFP) Conference

standards committees

2024-Now	Invited Expert, W3C Privacy Working Group
2007-2008	Invited Expert, W3C Web Security Context (WSC) Working Group
2004-2006	Invited Expert, W3C Platform for Privacy Preferences (P3P) 1.1 Working Group

leadership roles

2024-Now	Advisory Board Member, Electronic Privacy Information Center (EPIC)
2016-Now	Research Director, ICSI Usable Security & Privacy Group
2012-Now	Director, Berkeley Laboratory for Usable and Experimental Security (BLUES)
2021-2023	Member, ICSI Scientific Leadership Council
2006-2008	Legislative Concerns Chair / Board of Directors, National Association of Graduate and Professional Students (NAGPS)
2006-2008	Vice President for External Affairs, Carnegie Mellon Graduate Student Assembly

teaching

Fall 2019 — **Usable Privacy and Security** — University of California, Berkeley
Designed and taught a course as part of the School of Information's Masters in Cybersecurity program. Duties included course design and development, grading assignment and exams, supervising class projects, and holding office hours.

Spring 2017, Spring 2018 — **Human Factors in Computer Security and Privacy** — Brown University
Instructor for a module on "user interfaces for security" as part of the Executive Masters in Cybersecurity program. Duties included course design and development, grading assignments and exams, supervising thesis projects, and holding office hours.

Fall 2007 — **Information Security & Privacy (46-861)** — Carnegie Mellon University
Teaching assistant duties included developing course materials (topics for lectures, assignments, and exams), grading assignments and exams, holding office hours, and mentoring students about semester-long projects.

Spring 2006 — **Computers and Society (15-290)** — Carnegie Mellon University
Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, holding office hours, and mentoring students about semester-long projects.

Fall 2003 — **Information Security (CS 451)** — University of Virginia
Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, and holding office hours.

Fall 2003 — **Intellectual Property (TCC 200)** — University of Virginia
Teaching assistant duties included grading assignments and holding office hours.

Spring 2003, Spring 2004 — **Advanced Software Development Methods (CS 340)** — University of Virginia
Teaching assistant duties included grading and holding office hours.

Fall 2002 — **Engineering Software (CS 201J)** — University of Virginia
Teaching assistant duties included grading assignments and holding office hours.